CLAIMS

What is claimed is:

1. A communication system comprising:

a secure message generation system that employs a first dialog session key to encrypt a first message to be sent to a second service; and,

a secure message receiver system that employs a second dialog session key to decrypt a second message received from the second service.

2. The communication system of claim 1, the secure message generation system comprising:

a service pair encryption component that employs an initiator private key to encrypt authentication information;

a key exchange key encryption component that employs a target public key to encrypt a key exchange key;

a dialog session key encryption component that employs the key exchange key to encrypt the first dialog session key;

a message body encryption component that employs the first dialog session key to encrypt a message body of the first message to be sent to the second service; and,

a message generator that provides the encrypted first message to the second service, the encrypted first message being based, at least in part, upon the encrypted authentication information, the encrypted key exchange key, the encrypted first dialog session key and the encrypted message body.

3. The communication system of claim 2, the key exchange key comprising a symmetric key.

4. The communication system of claim 2, the key exchange key comprising a 128-bit symmetric key.

5. The communication system of claim 2, the key exchange key uniquely assigned to the service and second service pair.

6. The communication system of claim 1, the secure message receiver system comprising:

a message receiver that receives the encrypted second message;

a service pair encryption component that employs an initiator public key to decrypt authentication information of the encrypted second message;

a key exchange key decryption component that employs a target private key to decrypt a key exchange key of the encrypted second message, if the key exchange key is not stored in a cache;

a dialog session key decryption component that employs the key exchange key to decrypt the second dialog session key of the encrypted second message, if the second dialog session key is not stored in the cache; and,

a message body decryption component that employs the second dialog session key to decrypt a message body of the encrypted second message.

7. The communication system of claim 1, a value of the first dialog session key changed based, at least in part, upon a dialog session key policy.

8. The communication system of claim 7, the dialog session key policy is time-based.

9. The communication system of claim 7, the dialog session key policy is based, at least in part, upon a shift in the second dialog session key.

10. The communication system of claim 1, a dialog is failed based, at least in part, upon a dialog session key policy.

11. The communication system of claim 10, the dialog session key policy is based a quantity of shifts of the second dialog session key in a given time period.

12. The communication system of claim 10, the dialog session key policy is based, at least in part, upon a failure of shift of the second dialog session key in given time period,

13. A method facilitating secure communication comprising:

providing an encrypted first message of a dialog based, at least in part, upon a first dialog session key; and,

decrypting an encrypted second message of the dialog, decryption being based, at least in part, upon a second dialog session key.

14. The method of claim 13, the first dialog session key is changed based, at least in part, upon a dialog session key policy.

15. The method of claim 14, the dialog session key policy is time-based.

16. The method of claim 14, the dialog session key policy is based, at least in part, upon a shift in the second dialog session key.

16. The method of claim 14, the dialog session key policy is based a quantity of shifts of the second dialog session key in a given time period.

18. The method of claim 14, further comprising providing an encrypted first dialog session key, the encryption being based, at least in part, upon a key exchange key.

19. A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 13.

20. A data packet transmitted between two or more computer components that facilitates secure communication, the data packet comprising:

a key exchange key header comprising an encrypted key exchange key;

a dialog session key header comprising a first dialog session key encrypted with the key exchange key; and,

a message body field comprising a message encrypted with the first dialog session key, the data packet received by a service that employs a second dialog session key to encrypt a message the service originates.

21. A computer readable medium storing computer executable components of a communication system, comprising:

a secure message generation system component that employs a first dialog session key to encrypt a first message to be sent to a second service; and,

a secure message receiver system component that employs a second dialog session key to decrypt a second message received from the second service.

22. A communication system comprising:

means for generating a secure first message employing a first dialog session key to encrypt a first message to be sent to a second service;

means for receiving a secure second message from the second service; and,

means for decrypting the second message employing a second dialog session key.